AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A data processing apparatus having a secure domain and a non-secure domain, in the secure domain devices of the data processing apparatus having access to secure data which is not accessible in the non-secure domain, the data processing apparatus comprising:

a device bus;

a plurality of devices ~~device~~ coupled to the device bus, ~~and~~ each operable to issue a memory access request pertaining to either said secure domain or said non-secure domain at least one of the devices being operable in a plurality of modes, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain; and

a memory coupled to the device bus and operable to store data required by the devices~~device~~, the memory comprising secure memory for storing secure data and non-secure memory for storing non-secure data;

each ~~the~~ device being operable to issue onto the device bus the memory access request when an access to an item of data in the memory is required, the memory access request issued by the device including a domain signal identifying whether the memory access request pertains to said secure domain or said non-secure domain, and the domain signal being provided for use in determining whether the access defined by the memory access request is allowed to proceed.

2. (Currently Amended) A data processing apparatus as claimed in Claim 1, wherein for said at least one of the devices, said ~~the device is operable in a~~ plurality of modes are replicated in said~~, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the~~ secure domain and said non-secure domain.

3. (Currently Amended) A data processing apparatus as claimed in Claim 1, wherein the devices~~device has~~ have a predetermined pin for outputting the domain signal onto the device bus.

4. (Currently Amended) A data processing apparatus as claimed in Claim 1, wherein in said non-secure domain said at least one of the devices ~~device~~ is operable under the control of a non-secure operating system, and in said secure domain said at least one of the devices ~~device~~ is operable under the control of a secure operating system.

5. (Currently Amended) A data processing apparatus as claimed in Claim 1, further comprising partition checking logic coupled to the device bus and operable whenever the memory access request as issued by one of the devices ~~device~~ pertains to said non-secure domain to detect if the memory access request is seeking to access the secure memory, and upon such detection to prevent the access specified by that memory access request.

6. (Currently Amended) A data processing apparatus as claimed in Claim 5, wherein the partition checking logic is managed by one of the devices ~~device~~ when operating in a predetermined secure mode in said secure domain.

7. (Original) A data processing apparatus as claimed in Claim 5, wherein the partition checking logic is provided within an arbiter coupled to the device bus to arbitrate between memory access requests issued on the device bus.

8. (Currently Amended) A data processing apparatus as claimed in Claim 1, wherein said at least one of the devices ~~device~~ is a chip incorporating a processor, the chip further comprising a memory management unit operable, when the processor generates the memory access request, to perform one or more predetermined access control functions to control issuance of the memory access request onto the device bus.

9. (Original) A data processing apparatus as claimed in Claim 8, wherein the chip further comprises:

further memory coupled to the processor via a system bus, the further memory operable to store data required by the processor, the further memory comprising secure further memory for storing secure data and non-secure further memory for storing non-secure data; and

further partition checking logic coupled to the system bus and operable whenever the memory access request is generated by the processor when operating in a non-secure mode in said non-secure domain to detect if the memory access request is seeking to access either the secure memory or the secure further memory, and upon such detection to prevent the access specified by that memory access request.

10. (Currently Amended) A method of accessing a memory in a data processing apparatus having a secure domain and a non-secure domain, in the secure domain devices of the data processing apparatus having access to secure data which is not accessible in the non-secure domain, the data processing apparatus comprising a device bus, a plurality of devices ~~device~~ coupled to the device bus, each ~~and~~ operable to issue a memory access request pertaining to either said secure domain or said non-secure domain, at least one of the devices being operable in a plurality of modes, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain and a memory coupled to the device bus and operable to store data required by the devices~~device~~, the memory comprising secure memory for storing secure data and non-secure memory for storing non-secure data, the method comprising the steps of:

(i) issuing from any of the devices ~~device~~ onto the device bus the memory access request when an access to an item of data in the memory is required; ~~and~~

(ii) including within the memory access request a domain signal identifying whether the memory access request pertains to said secure domain or said non-secure domain; and

(iii) using the domain signal to determine whether the access defined by the memory access request is allowed to proceed.

11. (Currently Amended) A method as claimed in Claim 10, wherein for said at least one of the devices, said plurality of modes are replicated in said secure domain and said non-secure domain~~the device is operable in a plurality of modes, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain~~.

12. (Currently Amended) A method as claimed in Claim 10, wherein the devices ~~device has~~ have a predetermined pin for outputting the domain signal onto the device bus.

13. (Currently Amended) A method as claimed in claim 10, wherein in said non-secure domain said at least one of the devices~~device~~ is operable under the control of a non-secure operating system, and in said secure domain said at least one of the devices~~device~~ is operable under the control of a secure operating system.

14. (Currently Amended) A method as claimed in claim 10, further comprising the steps of:

(iii) whenever the memory access request as issued by one of the devices ~~device~~ pertains to said non-secure domain, employing partition checking logic coupled to the device bus to detect if the memory access request is seeking to access the secure memory; and

(iv) upon such detection, preventing the access specified by that memory access request.

15. (Currently Amended) A method as claimed in Claim 14, wherein the partition checking logic is managed by one of the devices~~device~~ when operating in a predetermined secure mode in said secure domain.

16. (Original) A method as claimed in Claim 14, wherein the partition checking logic is provided within an arbiter coupled to the device bus to arbitrate between memory access requests issued on the device bus.

17. (Currently Amended) A method as claimed claim 10, wherein said at least one of the devices~~device~~ is a chip incorporating a processor, the chip further comprising a memory management unit, when the processor generates the memory access request, the method comprising the step of:

employing the memory management unit to perform one or more predetermined access control functions to control issuance of the memory access request onto the device bus.

18. (Original) A method as claimed in Claim 17, wherein the chip further comprises further memory coupled to the processor via a system bus, the further memory operable to store data required by the processor, the further memory comprising secure further memory for storing secure

data and non-secure further memory for storing non-secure data, and further partition checking logic coupled to the system bus, the method further comprising the steps of:

whenever the memory access request is generated by the processor when operating in a non-secure mode in said non-secure domain, employing the further partition checking logic to detect if the memory access request is seeking to access either the secure memory or the secure further memory; and

upon such detection, preventing the access specified by that memory access request.

19. (Canceled).

20. (Canceled).